UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/540,501	06/23/2005	Patrice Hameau	HAMEAU2	2706

1444 7590 01/07/2008

BROWDY AND NEIMARK, P.L.L.C.
624 NINTH STREET, NW
SUITE 300
WASHINGTON, DC 20001-5303

EXAMINER	
CHEN, SHIN HON	
ART UNIT	**PAPER NUMBER**
2131	

MAIL DATE	DELIVERY MODE
01/07/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/540,501	HAMEAU ET AL.	
	Examiner	Art Unit	
	Shin-Hon Chen	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 November 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,13-15 and 17-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,13-15 and 17-21* is/are rejected.

7)☒ Claim(s) *17* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1, 13-15, and 17-21 have been examined.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 9/19/07 has been entered.

Drawings

3. The subject matter of this application admits of illustration by a drawing to facilitate understanding of the invention. Applicant is required to furnish a drawing under 37 CFR 1.81(c). No new matter may be introduced in the required drawing. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d).

Claim Objections

4. Claim 17 is objected to because of the following informalities: claim 17 discloses the method of claim 14 yet the limitations disclosed in claim 17 (e.g. "the aforesaid first mode for realizing" and "the test") seem to depend on limitations of claim 15. The examiner will examine

claim 17 as it depends on claim 15. Therefore, applicant is advised to amend the dependency of claim 17 from claim 14 to claim 15.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1, 13-15, and 17-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Griffin et al. U.S. Pat. No. 5249294 (hereinafter Griffin) in view of Kocher et al. U.S. Pub. No. 20020124178 (hereinafter Kocher).

7. As per claim 1, Griffin discloses a method for securing a computer system which comprises at least a code execution module (Griffin: figure 1: CPU) and memory capacities (Griffin: figure 1: ROM 18 and RAM 24) for storing interpreted code (Griffin: figure 1: Routines n-1...n) having measurable physical imprints (Griffin: column 1 lines 30-34: external observable event...change of voltage or current) wherein in order to make more difficult attacks based on physical measurements or requiring synchronization with said interpreted code (Griffin: column 1 lines 15-20: clock attack/differential power analysis attack), the method comprises the steps of:

providing at least two different implementations (Griffin: column 1 lines 46-49: randomly varying duration of predetermined routine creates different implementation) for at least one instruction of said interpreted code (Griffin: figure 1: predetermined routine comprises

routines n-1, n, n+1, ..., etc), said different implementations each requiring a different execution time and/or having a different physical imprint (Griffin: column 1 lines 46-49: randomizing the duration of program executions to change the power fluctuation) while providing an identical result (Griffin: column 1 line 47: randomizing duration of execution does not result in change of result);

selecting one of said different implementations to be executed before each execution of said instruction (Griffin: column 1 lines 61-62: assembling m of n interim subroutines through random selection to be included in one implementation of predetermined routine/interpreted code); and

executing the determined different implementation (Griffin: column 1 lines 55-50: executing the determined implementation).

Griffin discloses executing routines/instructions by a processor (Griffin: figure 1: routines/interpreted code). Griffin does not explicitly the system comprises a code interpretation module. However, Kocher discloses a method of minimizing the effect of differential power analysis attack on a system that runs interpreted code (Kocher: [0058] line 20: running interpreted code as Java requires interpreting module on system). It would have been obvious to one having ordinary skill in the art to have a code interpretation module on a microprocessor system such as smartcard because it is well known in the art to execute instructions (machine code) that are interpreted from high-level language and both prior art disclose a microprocessor that protects data from differential power analysis attack by introducing additional instructions. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Kocher within the system of Griffin because

code interpretation module allows different high-level language programs to be executed in a single platform.

8. As per claim 13, Griffin as modified discloses the method according to claim 1. Griffin as modified further discloses the method comprising:

a first mode for introducing a plurality of implementations of certain instructions consisting of enriching the set of instructions recognized by the interpreter with a plurality of implementations for a given instruction (Griffin: column 61-64: assembling interim routines to be included for program execution; column 3 lines 37-39: assembling interim routines enriches the set of instructions by embedding instructions into the interim routines).

9. As per claim 14, Griffin as modified discloses the method according to claim 1. Griffin as modified further discloses the method comprising:

a second mode for introducing the aforesaid plurality of implementations of certain instructions consisting of comprising in the actual implementation of the instruction, a branching to a portion of at least one alternative code with a variable physical imprint or duration, which dynamically determines the implementation to be executed (Griffin: figure 4 and column 6 lines 44-45: branch to interim routines; column 7 lines 4-14: the CPU executes interim routines randomly by following pointers to dynamically execute interim routines).

10. As per claim 15, Griffin as modified discloses the method of claim 14. Griffin as modified further discloses the method comprising:

a first mode for realizing the aforesaid alternative code consisting of proposing a plurality of different implementations of the instruction (Griffin: column 1 lines 61-64: randomly selecting and assembling m of n routines) and by conditioning the choice of the executed version to a dynamical test depending on data known at execution (Griffin: column 2 lines 31-33: monitoring the interim routines to detect whether the routines are tampered with).

11. As per claim 17, Griffin as modified discloses the method of claim 15. Griffin as modified further discloses the method comprising:

a second mode for realizing the aforesaid "alternative code" consisting of improving the aforesaid first mode for realizing "alternative codes" consisting of replacing the test for deciding on the selected version with a branching in an indirection table containing the addresses of the available version at an index calculated for variable items (Griffin: figure 4: the CPU uses table of pointers for interim routine to branch to respective interim routines selected; column 6 lines 4-12: the pointers allows the CPU to branch to respective randomly selected interim routines).

12. As per claim 18, Griffin as modified discloses the method of claim 1. Griffin as modified further discloses the method being implemented on a module for interpreting software code, a so-called virtual machine (Kocher: [0058] line 20: Java interpreted code requires Java virtual machine in order to be compiled). Same rationale applies as in claim 1.

13. As per claim 19, Griffin as modified discloses the method of claim 18. Griffin as modified further discloses wherein said virtual machine is a Java platform (Kocher: [0058] line 20: Java platform).

14. As per claim 20, Griffin as modified discloses the method of claim 1. Griffin as modified further discloses the method being implemented on a module for interpreting physical code (Griffin: figure 1: the CPU executes the routines, which are low-level machine codes).

15. As per claim 21. Griffin as modified discloses the method of claim 1. Griffin as modified further discloses the method being implemented on an embedded system and on an interpretation module of the microcontroller or microprocessor type (Griffin: figure 1 and column 3 line 5: secure microprocessor; Kocher: figure 2: smartcard microprocessor).

Response to Arguments

16. Applicant's arguments with respect to claims 1, 13-15, and 17-21 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

17. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Liardet U.S. Pub. No. 20030101351 discloses method for countering differential power analysis by introducing branching operation to code sequences.

Kissell U.S. Pat. No. 6976178 discloses method for disassociating power consumed within a processing system with instructions it is executing.

Kaiserswerth et al. U.S. Pub. No. 20030093684 discloses method with reduced information leakage.

Pezeshki et al. U.S. Pub. No. 20020029346 discloses method for minimizing differential power analysis attacks on processors.

Anderson et al. U.S. Pub. No. 20030084336 discloses microprocessor resistant to power analysis.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shin-Hon Chen whose telephone number is (571) 272-3789. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Shin-Hon Chen
Examiner
Art Unit 2131